UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,223	08/28/2001	Hamid Asayesh	4906.P020	5681

8791 7590 04/06/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER
NGO, NGUYEN HOANG

ART UNIT	PAPER NUMBER
2663	

DATE MAILED: 04/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/941,223	**Applicant(s)** HAMID ASAYESH	
	Examiner Nguyen Ngo	**Art Unit** 2663	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-24 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-24 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed 8/28/2001 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Objections

2. Claim 13 and 14 are objected to because of the following informalities:
As for claim 13: The "apparatus of claim 11" in line 1 should be - apparatus of claim **12**-.
The Examiner believes that there might be a typographical error and that this claim might depend on claim 12. There is no apparatus mentioned in claim 11 and thus presumes claim 13 to depend on claim 12.

As for claim 14: The "apparatus of claim 11" in line 1 should be - apparatus of claim **12**-.
The Examiner believes that there might be a typographical error and that this claim might depend on claim 12. There is no apparatus mentioned in claim 11 and thus presumes claim 14 to depend on claim 12.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (U.S 2002/0163920) in view of Sakamoto et al. (U.S 6,633,571), hereinafter referred to as Walker and Sakamoto, respectively.

Regarding claim 1, Walker discloses a method for performing network routing, which first authenticates (key corresponding to a VPN, [0013]) received packets sent from a source agent to an endpoint of a tunnel (set of endpoints) by determining whether a security association or SA (in which the process of creating SA involves the establishment of a private key ([0012])), of a received packet corresponds to the source agent that sent the packet, the tunnel being configured by said source agent in accordance with a network protocol (establishing tunnel). The authenticated packet is then routed to the selected routing destination (processing a set of traffic for the VPN, [0029]).

Walker is however silent in stating the tunneling protocol to be GRE and merely states a VPN security protocol such as IPSec to be used.

Sakamoto discloses that VPN realized by the IPSec method cannot be protected from the attacks of malicious users who can crack code and in addition, the encoding processing becomes a bottleneck of increasing the speeds for fast networks and terminal costs are increased (col1 lines 40-46). Sakamoto further discloses that GRE encapsulation, IP mobile, and other methods may be used for encapsulating IP packets.

Sakamoto thus provides the motivation for using any encapsulation (GRE) protocol to decrease bottleneck and terminal costs. It is therefore obvious to a person skilled in the art to use the GRE protocol disclosed by Sakamoto with the method for performing network routing disclosed by Walker. The applicant has further supported the motivation of interchangeable tunneling protocols by stating, " the present invention can be implemented with another tunneling protocol similar to GRE " (pg7 [0024]). It is well known in the art that GRE and IPSec are typically used for the encapsulating protocol.

Regarding claim 2, Walker discloses that the sources 4 will be assumed to be an isolated network such as host computers and VLANS (pg. 5 [0042]) and isolated network 4 is authorized by contract to send packets over their tunnel only to isolated network 11 ([0044]). It is well known in the art that VLANS require the use of routers (first and fourth virtual router corresponding to the VPN). Walker further discloses that the tunnel endpoints are legitimate routing destinations ([0038]), comprising a router 20, that may be associated with IP addresses (second and third virtual routers corresponding to a backbone, endpoint 2 of figure 2 and [0045]).

Regarding claim 3, Walker discloses an SA that would provide a routing constraint: specifying that all packets at the ingress of tunnel E (initiation point and termination point for GRE tunnel) with source IP addresses (first subset of the set of endpoints for entering and exiting the VPN) within network 10.0.0. are to be routed to VLAN F ([0039]).

Regarding claim 4, arguments analogous to those stated in the rejection of claim 1 are applicable with further arguments corresponding to specific limitations of claim 4. Walker discloses that each IP packet arriving through tunnel X (first set of endpoints for GRE tunnel) is authenticated (key) and assuming the authentication is successful, a table is used to look up (use of key and first set of endpoints, indexed in table, to determine second set of endpoints for the VPN) the destination address which may be a VLAN address (second set of endpoints for the VPN), to which the packets may be routed (establishing the GRE tunnel and processing a set of traffic for the VPN, figure 4a and [0051]).

Regarding claim 5, Walker discloses that each IP packet arriving through tunnel X must be directed to destination Y, which is a layer 3 device (virtual routers being an initiation and termination point for the GRE tunnel, [0051]).

Regarding claim 6, Walker discloses that the sources 4 will be assumed to be an isolated network such as host computers and VLANS (pg. 5 [0042]) and isolated network 4 is authorized by contract to send packets over their tunnel only to isolated network 11 (first and second virtual router corresponding to the VPN, [0044]).

Regarding claim 7, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 8, arguments analogous to those stated in the rejection of claim 4 are applicable with further arguments corresponding to specific limitations of claim 8. The Examiner interprets the source agent 4 and tunnel end point 1 mentioned in claim 2 to be considered a first network element (figure 1). Walker further discloses the authenticated packet (having a SA or key with the source agent) is routed to the selected routing destination (transmit a packet having the first set of end points and the key, [0029]).

The Examiner interprets the isolated destination network 11 and tunnel end point 2 to be considered a second network element (figure 1) which is shown to be coupled with the first network element and to receive the packet (figure 2). Walker further discloses that if the table (included in the SA) specified that the packet required a routing header after the packet has arrived through the tunnel (receive packet and establish GRE tunnel), the appropriate IP header would be added to the packet before sending it along to its routing destination (second set of endpoints for the GRE VPN, [0051]).

Regarding claim 9, Walker meets all the limitation of claim 8 but is however silent in disclosing a third network element.

Sakamoto, however, discloses of an interwork router (third network element) that provides functions for determining the route to output packets (receive a set of data from first network element and forward to second network element) between networks with different Internet Service Providers or ISPs and thus connecting said ISPs to each other for a VPN (set of data being for the VPN, figure 3 and col3 lines 29-35). As shown in figure 3, the Examiner interprets the interwork router (third element) to be coupled with LAN 1 and edge node 3-1 (first network element) and LAN 3 and edge node 3-3 (second network element).

Sakamoto thus discloses that a VPN may use public networks that are comprised of a plurality of networks managed by different ISPs and gives the motivation to incorporate an interwork router (third element) to securely and correctively connect to endpoints for a VPN. It would have thus been obvious to a person skilled in the art to include a interwork router (third element) disclosed by Sakamoto into the method for securely performing network routing disclosed by Walker in order to ensure the connection of endpoints with a backbone comprising of different ISPs.

Regarding claim 10, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 11, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 12, Walker discloses an apparatus or router ([0045]) comprising an authentication logic, decision logic and routing logic. It should be obvious to a person skilled in the art that these logic or sequences of functions be performed by hardware or software (engine). The authentication logic (control engine) is configured to receive packets sent from a source agent (second set of endpoints corresponding to the first set of end points and a key) to a tunnel endpoint (first set of endpoints corresponding to GRE tunnel) and to determine whether or not a SA (key) of the packets corresponds to the source agent ([0028]).

Walker further discloses a decision logic (forwarding engine), which makes a routing decision (establish initiation point of tunnel) for each authenticated packet that is constrained based on the SA ([0028]) and a routing logic (forwarding engine) that selects a routing destination (transmit a set of traffic over the GRE VPN) based on the routing decision logic ([0028]).

Regarding claim 13, Walker discloses that tunnel endpoints comprise of routers as mentioned above. These routers are then comprised of said decision logic and routing logic (host a first virtual router corresponding to one of the first set of endpoints, [0045]). Walker further discloses that the decision logic (forwarding engine) makes a routing decision for each authenticated packet (host a second virtual router corresponding to one of the second set of endpoints ([0028]).

Regarding claim 14, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 15, arguments analogous to those stated in the rejection of claim 12 are applicable with further arguments corresponding to specific limitations of claim 15. As mentioned with claim 12, Walker discloses an authentication logic that is configured to receive packets sent from a source agent to a tunnel and to determine whether or not a SA of the packets corresponds to the source agent (receive set of data, a key corresponding to VPN, and first set of endpoints of a GRE tunnel [0028]). It should be obvious to a person skilled in the art that this authentication logic performs both functions of the input/output module and control engine.

Regarding claim 16, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 17, arguments analogous to those stated in the rejection of claim 4 (configure second set of endpoints to first set of endpoints) are applicable with further arguments corresponding to specific limitations of claim 17.

Walker is however silent to indicate the key in a list of keys. But it should be obvious to a person skill in the art that a Security Association Database or SAD contain parameters (list of keys) associated with each SA.

Regarding claim 18, arguments analogous to those stated in the rejection of claim 4 are applicable with further arguments corresponding to specific limitations of claim 18 (machine-readable medium). Walker discloses that the method in correlation to claim 4 be implemented in the form of software ([0058]). Walker further discloses that the computer program (method) be embodied on a computer readable medium (page 7 claim 24).

Regarding claim 19, arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 20, Walker discloses the isolated network 5 be authorized by contract to send packets over their tunnel only to isolated network 12 (second VPN, figure 1 and [0044]). It is inherent that the steps in configuring said second VPN, correlate to the steps in configuring the first VPN mentioned in claim 4. Thus arguments analogous to those stated in the rejection of claim 4 are applicable.

Regarding claim 21, arguments analogous to those stated in the rejection of claim 4 are applicable with further arguments corresponding to specific limitations of claim 17 (listening for a packet and receiving packet).

Walker discloses that the routing constraint mentioned with claim 4 could also be applied in reverse to permit packets to exit through the ingress of an outbound tunnel (listening for a packet and receiving the packet [0052]), the packet being authenticated (key) with tunnel endpoint X (packet indicating set of endpoints for GRE tunnel and key for VPN [0051]), and then routed to the IP address found in the table of SA (retrieving second set of endpoints for VPN with first set of endpoints and key, [0051]).

Regarding claim 22, arguments analogous to those stated in the rejection of claim 17 are applicable.

Regarding claim 23, arguments analogous to those stated in the rejection of claim 20 are applicable.

Regarding claim 24, Walker discloses that whenever a packet is received (receiving second packet) at an endpoint of the tunnel, an authentication process is performed which authenticates (second packet indicating a second key) the packet. If the authentication fails, the packet is discarded (determining the second key is not in a key list) ([0049]). Walker further discloses that the conventional routing technique of using an IP address within the payload packet to determine destinations may be combined with the methods disclosed with claim 4 ([0054]). Thus access control list rules may be applied to each tunnel packet (ensuring that the second packet originated from an interior source, [0057]).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) Adams et al. (U.S 2003/0016679) Method and Apparatus to Perform Network Routing.

b) Nguyen et al. (U.S 2002/0016926) Method and Apparatus For Integrating Tunneling Protocols with Standard Routing Protocols.

c) Pao et al. (U.S 6,694,437) System and Method For On-Demand Access Concentrator For Virtual Private Networks.

d) Larson (U.S 2002/0093915) Third Party VPN Certification.

e) Arrow et al. (U.S 6,226,751) Method and Apparatus For Configuring A Virtual Private Network.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nguyen Ngo whose telephone number is (571) 272-8398. The examiner can normally be reached on Monday-Friday 7am - 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ricky Ngo can be reached on (571) 272-3139. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

N.N.
***

Nguyen Ngo
United States Patent & Trademark Office
Patent Examiner AU 2663
(571) 272-8398

Ricky Ngo
RICKY NGO
PRIMARY EXAMINER
4/4/05